Client-side defenses against web-based identity theft

Students: Robert Ledesma, Blake Ross, Yuka Teraguchi

Faculty: Dan Boneh and John Mitchell

Stanford University

PORTIA Project
Phishing Attack

Spam email: “There is a problem with your eBay account.”

User clicks on email link to go to badguy.com.

User thinks it is ebay.com, and enters eBay username and password.

Information is sent to the bad guy.
Sample phishing email

Dear Earthlink User

The reason why you have received this letter again is that you didn’t provide us with your exact user account information as it was requested in our first letter. Please, fill in the forms carefully so that we could keep your account information up-to-date which would allow us to provide you with better services in the future.

https://www.start.earthlink.net/track?billing.asp

Thanks for using Earthlink.

Sincerely,
EarthLink Team.
Spoof page

http://202.69.39.30/snkee/....
Magnitude of problem

- Fastest growing crime on the Internet.

- Primary targets: attacks/month (2004)

<table>
<thead>
<tr>
<th></th>
<th>July</th>
<th>June</th>
<th>May</th>
<th>...</th>
<th>Jan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citibank</td>
<td>682</td>
<td>492</td>
<td>370</td>
<td>...</td>
<td>34</td>
</tr>
<tr>
<td>US Bank</td>
<td>622</td>
<td>251</td>
<td>167</td>
<td>...</td>
<td>2</td>
</tr>
<tr>
<td>eBay</td>
<td>255</td>
<td>285</td>
<td>293</td>
<td>...</td>
<td>51</td>
</tr>
</tbody>
</table>

http://www.antiphishing.org
Properties of Spoof Sites

- Ask for user input, e.g. password.
  - Some ask for CCN, SSN, mother’s maiden name, ...

- HTML copied from honest site
  - Contain links to the honest site
  - Logos from honest site.
    - Copied jpg/gif file, or link to honest site
  - Can contain revealing mistakes

- Clever spoof pages contain Javascript to fool user.

- Short lived
  - Blacklisting spoof sites has limited success.

- HTTPS uncommon
Thanks!

- Robert Rodriguez
- Chris Von Holt
- Alissa Cooper
- Tom Pageler
- Greg Crabb

Many more ...
What can we do about phishing?

- **Spam filter:**
  - Phishing starts with email, so stop it there.
  - Non-trivial: phishing emails look like ordinary email.

- **Browser-side methods (plug-ins)**
  - Detect spoof web site. Warn user.
  - Improve browser password management.

- **Server-side methods:**
  - Use strong user authentication instead of pwds.
    - User certificates or security tokens.

This talk: SpoofGuard
Our project at Stanford

Two browser plug-ins available for download:

- **SpoofGuard**:  
  - Alerts user when browser is viewing a spoofed web page.  
  - Uses variety of heuristics to identify spoof pages.

- **PwdHash**:  
  - Simple mechanism for improving password management by the browser.

Will SpoofGuard solve the phishing problem?

- As likely to end phishing as first virus scanner was to end viruses
- A new type of anomaly detection problem
SpoofGuard:
Detect Phishing Web Sites

http://crypto.stanford.edu/SpoofGuard
SpoofGuard Browser Plug-in

- **Compute spoof index:**
  - Weighted sum of several spoof measures
  - Depends on current page and history

- **Provides two forms of information:**
  - Passive stoplight in toolbar: green, yellow, red
  - Active pop-up when necessary
    - Stop outgoing information to malicious web site

- **Challenges:**
  - Must be easy for novice users.
  - Detect malicious pages
  - Minimize false alarms
Stateless Page Evaluation

- **URL Check:**
  - Similar to well known site
    - www.ebay-fixit.com
    - www.ebau.com
  - IP address instead of host name
    - http://123.123.123.123/
  - Other tricks
    - www.ebay.com@123.123.123.123
  - Use reverse DNS to find domain if IP address

- **Image Check:**
  - Is image associated with different domain in image-domain database
Stateless Page Evaluation II

◆ **Link Check:**
  • Run URL check on links on the page
  • If significant fraction fail, raise alert

◆ **Password Check:**
  • Pages with password field are more suspicious than the one without
  • HTTPS and certificate validation
Stateful Page Evaluation

- **History Check:**
  - Site is assumed OK if in user’s history file
  - Very important for false alarm rate

- **Domain Check:**
  - Is current domain “similar” to a domain in the history list?

- **Email Check:**
  - Suspicious if page is referred by email link
POST Data Evaluation

- Intercepts and checks POST data
  - Keep hashed <domain, user, password> triples
  - If known user & password are sent to different domain, raise alert level
  - Exception for search engines
  - High alert: warn user and allow to cancel operation

POST: user_name=ice&password=cream
PwdHash: Improved Pwd Mgmt

http://crypto.stanford.edu/PwdHash
The common pwd problem

- Web users use the same username/password at many sites.
  - Users use their banking pwd at low security sites.

- **The problem**: break-in to low security site reveals banking username/passwords.

- **Ideal solution**: strong auth. protocols (SecureID/PKI)
  - Unlike pwd, requires HW or has limited mobility.
A Simple Solution

- Browser plug-in that converts a user’s pwd into a unique pwd per site.

1. Locate all pwd HTML elements on page:
   ```html
   <INPUT TYPE=password NAME=pass>
   ```

2. Whenever focus leaves a password field, replace contents of field with
   \[\text{HMAC}_{\text{pwd}}(\text{domain-name})\]

3. Password hash is sent to web site instead of pwd.

- Protection against phishing:
  - Spoof site only sees hash of user’s pwd.
Plug-in Challenges

- Pwd reset after plug-in install
- Javascript attacks
- What salt to use in hash?
- How to encode resulting hash?
- When to compute hash?
- Internet Café
- Dictionary attacks

- **Design goal**: transparent to user.
Plug-ins continue to evolve and improve:

- Easier deployment and use.
- Proxy-based solutions (not browser plug-ins)
- Strengthen spoof page identification.
- Deployment through Mozilla and billeo.

http://crypto.stanford.edu/SpoofGuard
What is SpoofGuard?

Installing SpoofGuard on Internet Explorer using MSI:
1. Run the MSI installer from here
2. Restart your browser
3. Display the toolbar by right-clicking on a toolbar and selecting SpoofGuard or select View -> Toolbars -> SpoofGuard
SpoofGuard User Interface

- SpoofGuard is added to IE tool bar
  - User configuration
  - Traffic light
    - Report green, yellow, red alert level
  - Pop-up as method of last resort
Pwd Hashing - an old idea

- Hash pwd with realm provided by remote site:
  - HTTP 1.1 Digest Authentication
  - Kerberos 5

- Hash pwd with network service name:
  - Gabber, Gibbons, Matyas, Mayer [FC ’96]. Proxy.
  - Abadi, Bharat, Marais [PTO ’97]

- **Challenge:** implementing in a modern browser.
eBay Spoof Site

Sends password to phisher